UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/653,506	09/02/2003	Len L. Mizrah	AIDT 1004-1	3811

22470 7590 04/02/2008
HAYNES BEFFEL & WOLFELD LLP
P O BOX 366
HALF MOON BAY, CA 94019

EXAMINER	
ABRISHAMKAR, KAVEH	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
04/02/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/653,506	**Applicant(s)** MIZRAH, LEN L.
	Examiner KAVEH ABRISHAMKAR	**Art Unit** 2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 September 2003*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-75* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-75* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date *09/22/03, 11/28/06, 7/25/07*.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application

6) □ Other: _____.

DETAILED ACTION

1. This action is in response to the communication filed on September 2, 2003. Claims 1-75 were originally received for consideration. No preliminary amendments for the claims were received.

2. Claims 1-75 are currently being considered.

Information Disclosure Statement

3. Initialed and dated copies of Applicant's IDS form 1449, received 09/22/03, 11/28/06, and 7/25/07, are attached to this Office Action.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-17, 22-43, and 47-75 are rejected under 35 U.S.C. 102(e) as being anticipated by Cuccia et al. (U.S. Patent 6,151,676).

As to claim 1, Cuccia teaches:

A method for establishing a communication session on a communication medium between a first data processing station and a second data processing station having access to the communication medium, comprising:

receiving at the first station a request from the second station for initiation of a communication session (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

producing dynamic sets of session random symmetric encryption keys at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

after receiving said request, executing a plurality of exchanges of encrypted messages across said communication medium to mutually authenticate the first station and the second station, and to provide the encryption key to the second station for use in said communication session (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 2, Cuccia teaches:

The method of claim 1, wherein during said plurality of exchanges, said first and second stations use at least two shared secrets, which are shared between the first station and the second station, or between the first station and a user at the second station, without exchanging messages carrying said shared secrets via the communication medium (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 3, Cuccia teaches:

The method of claim 1, including mutual authentication based on at least two shared secrets, without exchanging messages carrying said shared secrets in any form via the communication medium (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 4, Cuccia teaches:

The method of claim 1, wherein said plurality of exchanges comprise interactive exchanges, said interactive exchanges including a message from the first station to the second station and a responsive message from the second station to the first station, where the responsive message comprises information from the message from the first station derived using information derived from a message in a previous exchange (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 5, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

assigning a session random key in said first station, in response to a request received by said first station during a session random key initiation interval for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

wherein said plurality of exchanges includes at least one message carrying an encrypted version of one of said plurality of intermediate data random keys to be accepted as said encryption key upon said mutual authentication (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 6, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

providing a buffer at the first station; generating keys and storing said keys in the buffer (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating respective session random key initiation intervals with said keys stored in said buffer (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

using keys from said buffer as session random keys in response to requests received by said first station during said respective session random key initiation intervals for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

removing keys from said buffer after expiry of the respective session random key lifetime in the buffer (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 7, Cuccia teaches:

The method of claim 6, wherein said buffer is managed as a circular buffer (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 8, Cuccia teaches:

The method of claim 6, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value of session random key lifetime to engage into establishing a communication session, where M is less than or equal to 10 (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27)

As to claim 9, Cuccia teaches:

The method of claim 6, wherein a session random key lifetime in the buffer for said plurality of exchanges has a value within which the plurality of exchanges can be completed in expected circumstances, and said keys are removed from said buffer after a multiple M times said value, and the session random key lifetime to engage into establishing a communication session is less than about 90 second (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 10, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

wherein said plurality of exchanges includes a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter, which is shared between the first station and the second station, or between the first station and a user at the second station, and encrypted using the session random key (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and decrypting the shared parameter from said second message at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 11, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

wherein said plurality of exchanges includes

a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station to validate the second station, or a user at the second station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and a second exchange including sending a further message from the first station to the second station, the further message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns another message carrying a hashed version of said particular data random key encrypted using said particular encryption key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim12, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least one shared secret (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 13, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

after said request for initiation of a communication session, presenting to the second station a user interface along with the session random key, said user interface including a prompt for entry of a shared parameter and at least two shared secrets (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 14, Cuccia teaches:

The method of claim 1, wherein producing an encryption key at the first station includes:

assigning, in said first station, a session random key for use within a session random key initiation interval in response to requests received by said first station during said session random key initiation interval for use in a first exchange of said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

associating, in said first station, a plurality of intermediate data random keys with said request for use in said plurality of exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

wherein said plurality of exchanges includes a first exchange including sending a first message from the first station carrying said session random key to the second station, where the second station returns a second message carrying a shared parameter encrypted using the session random key, and decrypting the shared parameter at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

a second exchange including sending a third message from the first station to the second station, the third message carrying a particular data random key from said plurality of intermediate data random keys encrypted using the session random key, where the second station returns a fourth message carrying a hashed version of said particular data random key encrypted using said particular data random key to the first station, and decrypting said hashed version of said particular data random key at the first station using said particular data random key (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and then executing at least one additional exchange in said plurality of exchanges,

where said at least one additional exchange includes sending an additional message from the first station to the second station carrying a next data random key from the plurality of intermediate data random keys associated with said request, encrypted using a key exchanged during a previously completed exchange in said plurality of exchanges, where the second station decrypts said next data random key and returns a responsive message carrying a hashed version of said next data random key encrypted using said next data random key, and decrypting at the first station said hashed version of said next data random key using said next data random key (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 15, Cuccia teaches:

The method of claim 14, including during at least one of said additional exchanges, producing said third message by first veiling the particular data random key using a first conversion array seeded by a first shared secret and encrypting the veiled particular data random key, where the second station decrypts and unveils said particular data random key using the first shared secret, and where the second station produces said fourth message by veiling the hashed version of the particular data random key using a second conversion array seeded by said first shared secret and encrypting the veiled hashed version of the next data random key (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

decrypting and unveiling the hashed version of the particular data random key at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 16, Cuccia teaches:

The method of claim 14, including executing more than one of said additional exchanges (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 17, Cuccia teaches:

The method of claim 14, including during at least one of said additional exchanges, producing said additional message by first veiling the next data random key using a first conversion array seeded by a shared secret and encrypting the veiled next data random key, where the second station decrypts and unveils said next data random key using the shared secret, and where the second station produces said responsive message by veiling the hashed version of the next data random key using a second conversion array seeded by said shared secret and encrypting the veiled hashed version of the next data random key (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

decrypting and unveiling the hashed version of the next data random key at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 22, Cuccia teaches:

The method of claim 17, including upon request for initiation of a communication session, presenting to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 23, Cuccia teaches:

The method of claim 15, including upon request for initiation of a communication session, presenting to the second station a user interface for initiation of an authentication session including a compiled version of the session random key and parameters for one or more conversion arrays, said user interface including a prompt for entry of the shared parameter, and at least said shared secret (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 24, Cuccia teaches:

The method of claim 14, including executing a further exchange including sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

As to claim 25, Cuccia teaches:

The method of claim 14, including executing a further exchange including

sending a message from the first station to the second station carrying said encryption key encrypted using a first shared secret to the second station, where the second station returns a message carrying a hashed version of said encryption key encrypted using said first shared secret, and decrypting said encryption key at the first station (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27);

sending a message from the first station to the second station carrying said encryption key encrypted using a second shared secret, where the second station decrypts said encryption key, and returns a message to the first station carrying a hashed version of the encryption key encrypted using said second shared secret (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27); and

sending a message from the first station to the second station carrying an authentication signal indicating success or failure of mutual authentication and establishment of the encryption key, said authentication signal being encrypted using one of said intermediate data random keys from a previous exchange (column 3, lines 1-53, column 4, lines 3-30, column 4, lines 60-65, column 5, lines 20-27).

Claims 26-42, and 44-50 are apparatus claims analogous to the method claims of claims 1-17, and 22-25, and therefore, are rejected under the same rationale given above.

Claims 50-67 and 72-75 are article of manufacture claims analogous to the method claims of claims 1-17, and 22-25, and therefore, are rejected under the same rationale given above.

Allowable Subject Matter

Claims 18-21, 43-46, and 68-71 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Examiner, Art Unit 2131

/K. A./
03/28/2008
Examiner, Art Unit 2131